<u>REMARKS</u>

<u>REJECTIONS UNDER 35 U.S.C. § 112</u>

Claims 7-8, 23-24 and 39-40 were rejected under 35 U.S.C. § 112, second

paragraph, as being indefinite for failing to particularly point out and distinctly claim the

subject matter which Applicant regards as the invention. In particular, the Office action

states that the term "possible" is a relative term which renders the claims indefinite.

Claims 7, 23 and 39 have been amended to remove the term "possible" from the claims.

Thus, Applicant submits claims 7-8, 23-24 and 39-40 are definite and satisfy the

requirements of 35 U.S.C. § 112, second paragraph. Therefore, Applicant respectfully

requests the rejection of these claims be withdrawn.

<u>REJECTIONS UNDER 35 U.S.C. § 103</u>

<u>Claims 1, 4-6, 17, 20-22, 33 and 36-38</u>

Claims 1, 4-6, 17, 20-22, 33 and 36-38 were rejected under 35 U.S.C. § 103(a) as

being unpatentable over U.S. Patent No. 6,189,098 issued to Kaliski, Jr. (*Kaliski*) in view

of U.S. Patent No. 6,886,095 issued to Hind et al. (*Hind*). Applicant submits claims 1, 17

and 33 are not obvious in view of *Kaliski* and *Hind* for at least the reasons set forth

below.

Claim 1 recites, in part, the following:

> generating an authenticator string, the authenticator string
> demonstrating possession of a user terminal private key;

Claims 17 and 33 recite similar limitations.

The Office action correctly concedes that *Kaliski* does not teach or disclose

generating an authenticator string that demonstrates possession of a user terminal private

key, as recited in claim 1. The "Background of the Invention" section of *Kaliski* states

that with "public-key cryptosystems, it is computationally expensive to form digital signatures because of the need to perform an exponentiation operation." Col. 2, lines 57-59. Given the computational expense of digital signatures, the goal/purpose behind the invention/disclosure of *Kaliski* is to develop a server's trust in the client using a protocol that is less computationally expensive. See col. 3, lines 28-30. To that end, *Kaliski* specifically teaches against using a digital signature. See col. 3, lines 34-35.

Hind is cited as teaching an authenticator string that demonstrates possession of a user terminal private key. However, the cited portion of *Hind* discloses demonstrating possession of a private key by using a digital signature. See col. 12, lines 52-55; see also col. 8, lines 24-28. By citing *Hind*, the Office action is suggesting that *Kaliski* be modified to use a digital signature in an authenticator string to demonstrate possession of a user terminal private key. MPEP § 2143.01 states, in a salient part, the following:

> If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)

By citing *Hind* in combination with *Kaliski*, the Office action proposes a modification to *Kaliski* that would change the principle of operation in *Kaliski* (i.e., reducing computational expense by <u>not</u> using a digital signature). The suggested combination of *Kaliski* and *Hind* would require a substantial reconstruction and redesign of the elements shown in *Kaliski* as well as a change in the basic principle under which *Kaliski* was designed to operate. Therefore, Applicant respectfully submits the teachings of *Kaliski* and *Hind*, in combination, are not sufficient to render claims 1, 17 and 33 *prima facie* obvious.

Notwithstanding the lack of motivation to combine, even if *Hind* and *Kaliski* were combinable, the combination of *Hind* and *Kaliski* as cited fails to teach each and every element of the claims. Therefore, Applicant respectfully submits claims 1, 17 and 33 are not obvious in view of *Kaliski* and *Hind*.

Claims 4-6 depend from claim 1. Claims 20-22 depend from claim 17. Claims 36-38 depend from claim 33. Given that dependent claims necessarily include the limitations of the claims from which they depend, Applicant respectfully submits claims 4-6, 20-22 and 26-38 are not obvious in view of *Kaliski* and *Hind* for at least the same reasons claims 1, 17 and 33 are not obvious.

Claims 10-16, 26-32 and 42-48

Claims 10-16, 26-32 and 42-48 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Kaliski* in view of *Hind*. Applicant submits claims 10-16, 26-32 and 42-48 are not obvious in view of *Kaliski* and *Hind* for at least the reasons set forth below.

Claim 10 is a method claim that recites, in part, the following:

> receiving a message from a user terminal of the wireless access network, the message containing a shared secret encrypted with an access point public key, a user terminal certificate, and **an authenticator string demonstrating possession by the user terminal of a user terminal private key**;

Independent claims 26 and 42 are apparatus and Beauregard claims, respectively, that recite similar limitations.

Once again, the Office action correctly concedes that *Kaliski* fails to teach or disclose an authenticator string that demonstrates possession by the user terminal of a user terminal private key. In addition, as discussed above, *Hind* fails to cure the

deficiencies of *Kaliski* for at least the reason that the combination of *Kaliski* and *Hind* would require a modification to *Kaliski* that would change the principle of operation of *Kaliski* because *Hind* teaches the use of a digital signature while *Kaliski* specifically teaches against using a digital signature. Therefore, for at least the reasons set forth above, Applicant respectfully submits claims 10, 26 and 42 are not obvious in view of *Kaliski* and *Hind*.

Claims 11-16 depend from claim 10. Claims 27-32 depend from claim 26. Claims 43-48 depend from claim 42. Given that dependent claims necessarily include the limitations of the claims from which they depend, Applicant submits claims 11-16, 27-32 and 43-48 are not obvious in view of *Kaliski* and *Hind* for at least the same reasons discussed with respect to claims 10, 26 and 42.

NEW CLAIMS

Claim 49 has been added. Claim 49 depends from claim 17. Support for claim 49 can be found in paragraph [0026] of the specification. Applicant submits claim 49 is not obvious for at least the same reasons claim 17 is not obvious.
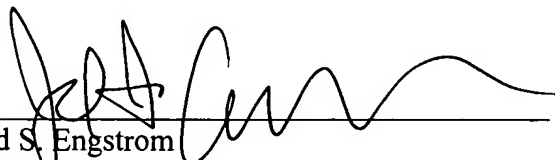
CONCLUSION

For at least the foregoing reasons, Applicant submits that the rejections have been overcome. Therefore, claims 1-48 are in condition for allowance and such action is earnestly solicited. The Examiner is respectfully requested to contact the undersigned by telephone if such contact would further the examination of the present application.

Please charge any shortages and credit any overcharges to our Deposit Account number 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Date: _1|10|07_

Jared S. Engstrom
Attorney for Applicant
Reg. No. 58,330

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1026
(503) 439-8778

CERTIFICATE OF MAILING:
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Kristin A. Morrow   1/10/07
_____   _____
Kristin A. Morrow   Date